

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FORTH WORTH DIVISION

CHANNEL (H), INC.,

Plaintiff,

v.

CQUENTIA SERIES, LLC;
HTG SERIES, a series declared by
CQUENTIA SERIES, LLC; and
D. ALAN MEEKER,

Defendants.

Case No.: 4:17-cv-00916-O

**REPLY MEMORANDUM OF LAW IN SUPPORT OF
MOTION FOR PRELIMINARY INJUNCTION**

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
PRELIMINARY STATEMENT	1
DISPUTED FACTS	1
ARGUMENT	6
A. Channel (H) Has Submitted Extensive Evidence That Defendants Misappropriated the Platform	6
B. Channel (H) Has Demonstrated That the Threat of Injury Outweighs Any Harm to the Defendants.....	11
C. Defendants’ Remaining Arguments Lack Merit.....	11
CONCLUSION	11

TABLE OF AUTHORITIES

Cases

<i>Am. Totalisator Co., Inc. v. Autotote Ltd.</i> , 1983 WL 21374 at *5 (Del Ch. Aug. 18, 1983).....	6
<i>Aspen Tech, Inc. v. M3 Tech, Inc.</i> , 569 Fed. Appx. 259, 267 (5th Cir. 2014).....	8
<i>Engenium Solutions, Inc. v. Symphonic Tech., Inc.</i> , 924 F.Supp.2d 757, 795-96 (S.D. Tex. 2013)	
.....	8
<i>GlobeRanger Corp. v. Software AG United States of Am., Inc.</i> , 836 F.3d 477, 498 (5th Cir. 2016)	
.....	7
<i>Miller v. Talley Dunn Gallery, LLC</i> , 2016 WL 836775 at *13 (Tex. Ct. App. Mar. 3, 2016)	6
<i>RealPage, Inc. v. Enter. Risk Control, LLC</i> , 2017 WL 3313729 (E.D. Tex. Aug. 3, 2017)	8, 9
<i>Spear Mktg., Inc. v. BanCorpSouth Bank</i> , 791 F.3d 586, 601 (5th Cir. 2015).....	7

Statutes

18 U.S.C. § 1836(b)(3)	6
------------------------------	---

Plaintiff, Channel (H), Inc. (“Channel (H)” or “Plaintiff”), by and through its undersigned counsel, hereby submits this Reply Memorandum of Law in further support of its Motion for a Preliminary Injunction.

PRELIMINARY STATEMENT

Defendants’ Response to Plaintiff’s Motion for Preliminary Injunction and Brief in Support (“Response”) fails to address critical facts and law raised on Plaintiff’s motion, and sets up a series of misleading arguments, which are either demonstrably false, implausible, or are controverted by Defendants’ own statements, pleadings, or public records. Defendants now claim that they determined that the Platform did not work in August 2017, however, as stated above, as late as August 28, 2017, Defendants sought a perpetual license of the Platform. Although Defendants have **admitted** in judicial pleadings that they have created a software-based pre-certification system, [Petition ¶¶ 24, 26], they now contend that their process was a “drastically different solution for pre-certifying patient approvals for the genetic testing services that CQ provides – a ***manual*** process. . .” Response at 1 (emphasis added); *see also* Declaration of Floyd L. Russell (“Russell Decl.”), ¶ 7. These claims are not only implausible, but are undermined by Defendants’ contradictory pleadings. For the foregoing reasons and the reasons stated below and in Plaintiff’s Memorandum of Law in Support of Motion for Preliminary Injunction (“Memorandum”), Plaintiff respectfully requests that its motion for a preliminary injunction be granted.

DISPUTED FACTS

CQ claims that it approached Channel (H) around the end of 2016 and beginning of 2017 and “inquired whether Channel (H), using CQ’s proprietary and trade secret process and data specifications, could develop a *fully-automated* software solution.” *See, e.g.*, [Response at 3, ¶ 6]. CQ’s claim is false – Plaintiff developed its Platform completely without Defendants’ input or

involvement. *See* Supplemental Declaration of Robert Capelli (“Supp. Decl.”) [Supp. Decl., ¶¶ 2-4]. First, there is no acknowledgement in any of the parties’ Agreements of any contribution by Defendants, whatsoever, to Plaintiff’s trade secret Platform. To the contrary, the Agreements universally state that the Platform is solely Plaintiff’s proprietary intellectual property. *See* June 2016 Agreement, Exhibit A, ¶ 3.3; October 2016 Agreement, Exhibit B, ¶¶ 20, 22, 31; January 2017 Agreement, Exhibit C, ¶¶ 3, 6; May 2017 NDA, Exhibit E. Verified Compl., ¶ 47. Moreover, Plaintiff presented its pre-certification functionality to Defendants at a meeting in June 2016 – six months before Defendants now judicially claim that they came up with the idea. [Supp. Decl., ¶ 4; **Exhibits L, M**].

Similarly, Defendants *never* complained about Plaintiff’s performance under the Agreements falling below any contractually-specified metric, as one might expect had the Platform truly not worked. [Supp. Decl., ¶¶ 5, 9(b), 9(c), 20; **Exhibit R**]. Nor do Defendants submit any evidence – aside from the internally inconsistent and implausible Russell Declaration – to support their claim that Channel (H)’s system did not work.

Although Defendants claim, on the one hand, that their “pre-authorization solution” is a “drastically different . . . manual process,” they state, on the other, that it is “not fully-automated.” [Response at 1, 4, ¶ 9]. Defendants provide scant details about what their solution is, or what “not fully automated” means. The Court may infer that “not fully-automated” means, “partially automated.” Indeed, in the Petition, Defendants call their preauthorization solution a “Preauthorization **Software** Solution.” [Petition, ¶¶ 24, 26] (emphasis added). Defendants, having already admitted to developing a software solution, simply expunged the word “software” from their Response, in a thinly-veiled attempt to obscure what their system actually is.

Defendants also misrepresent the scope of Channel (H)’s trade secrets. Significantly, although Defendants provide scant evidence of how their system works, one aspect of Defendants’ process – contacting insurance companies – is apparently manual, which is no different from Plaintiff’s process, which also involves manually contacting *some* insurance companies. [Supp. Decl., ¶¶ 9(g), 21, **Exhibit Y**]. Defendants *knew* this, and a screen capture of a file called, “Manual Process UCSD,” shared with Kenny Jones at CQ, proves it. [See **Exhibit Y**]. It is wholly disingenuous for Defendants to claim otherwise.

Defendants’ refusal to allow Plaintiff’s request to access Defendants’ Preauthorization Software Solution raised red flags, as Defendants had previously communicated to Plaintiff that they were “taking [his] system in house.” [Supp. Decl., ¶ 9(f); **Exhibit U**]. A week later, Defendants claimed that their system was completely manual. [Supp. Decl., ¶ 9(f)-(h); **Exhibit V**]. Given that the parties were subject to various non-disclosure, non-circumvention and confidentiality agreements, it was troubling that Defendants were unwilling to allow Plaintiff to confirm that their purported solution was not based on a breach of those agreements and a theft of Channel (H)’s trade secrets. In reality, Defendants were in talks to roll out the Platform to a number of hospital networks and insurance companies in deals worth hundreds of millions of dollars. [Supp. Decl., ¶ 9(d)(e), (k); **Exhibits S, T**]. Robert Capelli was actively involved in the integration process with these hospital networks. [*Id.*]. The idea that Defendants would replace the Platform with a manual process is laughable.

Plaintiff strongly disputes Defendants’ claim that the “Agreements do not preclude CQ and HTG from developing and implementing their own preauthorization solution.” [Response at 5, ¶ 12]. That is *exactly* what the Agreements prohibit. The Agreements contain numerous prohibitions barring unauthorized use, copying, disclosure, or circumvention of Plaintiff’s

proprietary intellectual property rights and trade secrets – in other words, developing and implementing a system based on Plaintiff’s trade secret software Platform and process. *See* June 2016 Agreement, Exhibit A, ¶¶ 3.2, 3.3; October 2016 Agreement, Exhibit B, ¶¶ 20, 22, 31; January 2017 Agreement, Exhibit C, ¶ 2(i), 3, 5(a); *see also* May 2017 NDA, Exhibit E. Verified Compl., ¶¶ 15, 47. Moreover, even if Defendants did contribute, *inter alia*, ideas, suggestions or code to Channel (H), any rights that Defendants could have had were expressly assigned to Channel (H). [October 2016 Agreement, **Exhibit B**, ¶¶ 31].

Defendants next argue that, because Plaintiff has not seen their system – which Defendants have refused to allow Plaintiff to see – that Plaintiff cannot have a claim for misappropriation. [Response at 7, ¶¶ 16-17]. This is completely unfounded and without any basis in law.

Defendants built their “Preauthorization Software Solution” shortly after receiving access to Plaintiff’s Github Account, which contained the code and work flow diagrams for building Plaintiff’s Platform. Additionally, Robert Capelli *flew* to Memphis on June 6 at Floyd Russell’s invitation to discuss the Platform. During that visit, Robert Capelli showed Floyd Russell and Ken Jones the admin platform, which is the back end of Channel (H)’s Platform. Put another way, it is the operating system of Channel (H) – it shows all of the data that is available, all of the connections to that data, and the intelligence run across that data (e.g., authorizations, certification, eligibility). [Supp. Decl., ¶¶ 18, 19; **Exhibit X**]. Moreover, Defendants were given access to and had discussions concerning what was in the admin panel. In February 2017, Robert Capelli emailed a .pdf of roughly 20 pages from the admin panel to Floyd Russell, Kenny Woods, Alan Meeker, and Jamison Feramisco of CQ, in advance of a meeting to go over the admin panel. [Supp. Decl., ¶ 19; **Exhibit Y**]. In other words, it is wholly disingenuous for Defendants to claim that they were not provided with access to Plaintiff’s trade secrets. Given the above, Plaintiff cannot simply take

Defendants' word for it that they did not misappropriate any part of Plaintiff's trade secrets. [e.g., Response, p. 7, ¶ 17; Russell Decl., ¶ 4 ("I never viewed the admin panel")].

The Russell Declaration is not credible

Floyd Russell makes a number of factually inconsistent, implausible and eyebrow-raising claims in his Declaration. First, he claims that once he learned that the source code was written in Ruby on Rails™, he: "had no desire to and did not view any additional source code files within the Github Account because. . .[he] knew that code written in Ruby on Rails was incapable of scaling or meeting the performance needs projected by CQ." Russell Decl., ¶ 4. Mr. Russell then claims that he "**never viewed the admin panel** or workflow documents allegedly uploaded to the Github account." *Id.* (emphasis added). Mr. Russell's claims are specious.

As stated above, shortly after the parties had signed the Term Sheet on May 16, 2017, and Mr. Russell viewed the Github Account on May 22, Robert Capelli flew to Memphis at Mr. Russell's invitation, and *showed* him the admin panel. [Supp. Decl., ¶¶ 18, 19; **Exhibit N**]. If Mr. Russell determined on or around May 22, 2017, that Channel (H)'s solution did not meet CQ's requirements, because it was built on Ruby on Rails, it is not clear why he proceeded to "work[] closely with Channel (H) in its attempted development and implementation of the Platform" through the end of August 2017. [Russell Decl., ¶ 5]. If Mr. Russell had truly believed that Ruby on Rails did not scale to CQ's needs, it would have made no sense for him to spend the next three months attempting to implement the Platform.

Mr. Russell never complained about Channel (H)'s use of Ruby on Rails, as a programming language, and never voiced any concerns as to the functionality, performance, or scalability of the Platform at any time until this litigation. [Supp. Decl., ¶¶ 5, 20; **Exhibit R**]. Moreover, the claim that Channel (H)'s Platform was developed "using CQ's proprietary trade secret process and data

specifications,” is also false. [Russell Decl., ¶ 5]. Channel (H) pitched the entire functionality of the Platform during its preliminary presentation to Defendants in May 2016. [Supp. Decl., ¶¶ 2-4; **Exhibits L, M**].

Mr. Russell next claims that after the Platform failed to work, he “began developing a completely different preauthorization solution.” [Russell Decl., ¶ 6]. He defines this as the “Preauthorization Solution.” Conspicuously missing from this defined term is the word “Software.” Although Mr. Russell claims, on the one hand, that he was forced to develop his own Preauthorization Solution because the Platform *automation* did not work properly, he contends, on the other, that the “Preauthorization Solution is completely different from the Platform in that coverage determinations are now performed *manually* by a full-time staff of CQ employees.” [Russell Decl., ¶ 6] (emphasis added). As stated above, Mr. Russell’s Declaration is so riddled with factual inconsistencies and implausible statements, as to be wholly unbelievable.

ARGUMENT

A. Channel (H) Has Submitted Extensive Evidence That Defendants Misappropriated the Platform

As an initial matter, Defendants’ opposition brief misstates the applicable legal standard. Both the Defend Trade Secrets Act and the Delaware Uniform Trade Secrets Act provide for an injunction when there is threatened misappropriation of a trade secret *See* 18 U.S.C. § 1836 (court may grant preliminary injunction “to prevent any actual or **threatened** misappropriation”) (emphasis added); *Miller v. Talley Dunn Gallery, LLC*, 2016 WL 836775 at *13 (Tex. Ct. App. Mar. 3, 2016) (“[T]he UTSA provides that the actual or threatened misappropriation of a trade secret may be enjoined.”); *Am. Totalisator Co., Inc. v. Autotote Ltd.*, 1983 WL 21374 at *5 (Del Ch. Aug. 18, 1983) (noting, under Delaware law, courts may enjoin threatened misappropriation of a trade secret).

Further, any exploitation of a trade secret that is likely to result in injury to the trade secret is a “use.” “Use” can be found where the exploitation includes “relying on the trade secret to assist or accelerate research or development.” *GlobeRanger Corp. v. Software AG United States of Am., Inc.*, 836 F.3d 477, 498 (5th Cir. 2016) (citation committed). “[P]roof of the defendant’s knowledge of the trade secret together with substantial similarities between the parties’ products or processes may justify an inference of use by the defendant.” *Spear Mktg., Inc. v. BanCorpSouth Bank*, 791 F.3d 586, 601 (5th Cir. 2015).

The Agreements between the parties clearly state that Channel (H) owns all rights in its proprietary trade secrets, software, process, and information. *See* Memorandum at 6-7. Defendants promised not to copy, make derivative works in or otherwise duplicate or create a system that performed the same function as Plaintiff’s system. *See* Memorandum at 6. Further, any conceivable rights that Defendants might possibly have claimed were expressly assigned to Channel (H). [October 2016 Agreement, **Exhibit B**, ¶¶ 31]. It is equally clear, however, that Defendants have violated these contractual safeguards.

Defendants were provided with access to Channel (H)’s proprietary technology pursuant to the May 2017 NDA and Term Sheet between the parties. [Verified Compl., ¶ 38; Russell Decl. at ¶ 4; Supp. Decl., ¶¶ 4, 5, 18, 19; **Exhibits L, M, N, X**]. Indeed, Mr. Russell admits that he accessed Channel (H)’s Github Account, which contained all code, admin panel and workflow documents for the Platform. Russell Decl. at ¶ 4. Less than a month after discussions between the parties on a perpetual license ended, Defendants launched an extremely similar and competing pre-authorization software product – even though it took Channel (H) over a year and a half to develop its own Platform. [Supp. Decl., ¶¶ 10-17]. In similar circumstances, courts have not hesitated to find misappropriation. *See Aspen Tech, Inc. v. M3 Tech, Inc.*, 569 Fed. Appx. 259, 267 (5th Cir.

2014) (noting that “evidence of a similar product may give rise to an inference of actual use under certain circumstances” and upholding a jury verdict of misappropriation of trade secrets when defendant had access to plaintiff’s trade secret and defendant developed a similar product *six months* later); *Engenium Solutions, Inc. v. Symphonic Tech., Inc.*, 924 F.Supp.2d 757, 795-96 (S.D. Tex. 2013) (granting summary judgment and finding misappropriation when defendant created a similar product shortly after one of plaintiff’s former employees joined defendant’s company). Tellingly, Defendants’ opposition papers provide no factual support as to how it was able to develop its product in such a short amount of time. The Russell Declaration merely states that he, “used his twenty years of experience” to create Defendants’ pre-authorization solution in a month, which is not credible, given the impossibly short time frame for development. [Russell Decl. at ¶ 6]. Defendants’ failure to provide *any* details as to how they created their product in such a small window further supports the inference that Defendants utilized Channel (H)’s trade secrets to create, or assist or accelerate the development, their Preauthorization Software Solution.

Defendants attempt to avoid the consequences of their misappropriation by citing to several cases standing for the proposition that merely providing access to an alleged trade secret, in and of itself, cannot be the basis for misappropriation of a trade secret. Those cases are inapposite. Defendants’ argument ignores the fact that Channel (H) has established more than just access to its trade secrets – Channel (H) has submitted evidence demonstrating that Defendants also *used* that access to accelerate their development of a competing product with identical functionality. [Verified Compl., ¶ 38; Russell Decl. at ¶ 4; Supp. Decl., ¶¶ 4, 5, 18, 19; **Exhibits L, M, N, W**].

RealPage, Inc. v. Enter. Risk Control, LLC, 2017 WL 3313729 (E.D. Tex. Aug. 3, 2017), cited by Defendants, actually supports Channel (H)’s argument. In that case, the plaintiff had little evidence that the defendant had actually-used its source code or trade secret materials. *See id.* at

*11. However, the plaintiff argued that use could be presumed, in part, because the defendant quickly developed a competing and similar code and the court agreed. *Id.* (“Use can [also] be found where the exploitation includes relying on the trade secret to assist or accelerate research or development.”) (internal quotations and citations omitted).

Defendants’ opposition brief also blatantly mischaracterizes the nature of the evidence offered by Channel (H) as “conclusory allegations.” To the contrary, Channel (H) has submitted verified pleadings, sworn declarations, and documentary evidence, supplemented herein, establishing that: (i) Channel (H) provided Defendants’ Chief Technology Officer and CEO with its code and proprietary businesses processes [Verified Compl., ¶ 38; Russell Decl. at ¶ 4; Supp. Decl., ¶¶ 4, 5, 18, 19; **Exhibits L, M, N, W**]; (ii) that on May 22, 2017, Floyd Russell accessed the Github (which contained all code for Channel (H)’s platform, admin panel and workflow documents [Verified Compl., ¶ 38; Russell Decl. at ¶ 4]; (iii) in February and June of 2017, Robert Capelli gave Defendants’ .pdf’s and presentations reflecting much of the functionality that Defendants have claimed is in their product [Supp. Decl., ¶¶ 4, 18-19; **Exhibits L, M, X, Y**], (iv) on August 29, 2017, Mr. Russell told Robert Capelli that Defendants were taking Channel (H)’s solution “in-house,” and admitted that Defendants’ pre-authorization solution receives a Schedule API before the qualifying events, filters out the insurance identifiers to call coverage against and provides nurses with a list of results that can printed for the day—which is identical to what Channel (H) was providing for Defendants [Verified Compl., ¶¶ 45, 46; Supp. Decl., ¶ 9(c)-(i); **Exhibits U, V**]; and (v) Plaintiff confirmed from a contact at CQ that CQ was still receiving the pre-certifications through an automated system *after* Defendants cut off Plaintiffs’ SRF. [Supp. Decl., ¶ 22].

Moreover, in the Verified Complaint and Declarations, Robert Capelli relies on his *personal* knowledge of the above-referenced events. [Verified Complaint, ¶¶ 45, 46]. Such evidence clearly rises above “conclusory allegations” and provides the Court with a clear timeline of Defendants’ misappropriation.

Finally, Defendants repeatedly argue that there has been no misappropriation because its product is “manual” and Channel (H)’s product is automated. As stated above, this argument is disingenuous, as Defendants’ solution also relies on *software*, and also because Channel (H) has always provided a manual option as one way of getting patient results to post. [Supp. Decl., ¶¶ 9(g), 21, **Exhibit Y**]. It is also relevant that log records demonstrate that Defendants were continuing to access Channel (H)’s Platform after September 18, and at least until **September 28, 2017**, although it had allegedly developed its own “manual” process by then. [Supp. Decl., ¶ 22; **Exhibit G**]. Notably, Defendants purportedly terminated the license agreements between the parties **two days earlier** on September 26, 2017, yet continued to use an automated system through September 28, when Plaintiff was completely shut out of the UCSD interface. **Exhibit G**.

Defendants’ argument also ignores the applicable legal standard. The standard for finding use of a trade secret is not whether defendant’s product contains plaintiff’s trade secrets but whether the defendant relied on plaintiff’s trade secret to assist or accelerate research of its product. *See Wellogix, Inc.*, 716 F.3d 867 at 877 (rejecting defendant’s argument that no misappropriation had occurred because defendant’s product lacked certain “dynamic” features when there was evidence and testimony that defendant relied on plaintiff’s trade secrets to create its product). The fact that Defendants were able to create a competing pre-authorization software solution in less than a month (and have provided *no* details as to how they could create a product so quickly), gives rise to an inference that they used Channel (H)’s trade secret to create their product,

especially in light of Defendants' access to Channel (H)'s Platform, process documents, and source code. Defendants' myriad of inconsistent and implausible explanations only strengthens that inference.

B. Channel (H) Has Demonstrated That the Threat of Injury Outweighs Any Harm to the Defendants

In light of Defendants' blatant theft of the Platform, the balance of hardships weighs in favor of Channel (H). Defendants' primary business is functioning as a diagnostic laboratory, not a software development company. Defendants can continue to operate their business without using the Platform (as Defendants previously did up until licensing Channel (H)'s technology and process in 2016).

Finally, if it turns out that Defendants' process truly does not incorporate any of Channel (H)'s proprietary information, the requested injunction will not harm Defendants. Channel (H)'s requested injunction *only* prohibits Defendants from using Channel (H)'s Platform or Confidential Information to build, develop, or create a service that replicates, performs the same functions as, or attempts to compete with Channel (H). If Defendant's pre-authorization product does not incorporate any of Channel (H)'s Platform or proprietary trade secret information, Defendants can continue business as usual.

C. Defendants' Remaining Arguments Lack Merit

Defendants do not rebut that Channel (H) has demonstrated there is a substantial threat of irreparable harm such that an injunction would serve the public interest, but instead rest their arguments on the incorrect assertion that Channel (H) has failed to demonstrate misappropriation of the Platform. Therefore, Defendants' remaining arguments in opposition lack merit.

CONCLUSION

For the reasons stated above, Plaintiff respectfully requests that this Court grant its motion for a preliminary injunction.

Dated: December 22, 2017

Respectfully submitted,

By: /s/ Brett E. Lewis

Brett E. Lewis

(*pro hac vice*)

Justin Mercer

(*pro hac vice forthcoming*)

Lewis & Lin, LLC

45 Main Street, Suite 608

Brooklyn, New York 11201

Tel. (718) 243-9323

brett@ilawco.com

justin@ilawco.com

THE APGAR FIRM, PLLC

MARGARET HORTON APGAR

State Bar No. 24036805

1914 Skillman Street, Suite 110-150

Dallas, Texas 75206

(214) 707-2791 (Phone)

(214) 279-6050 (Fax)

margaret@apgarfirm.com

Attorneys for Plaintiff

Of Counsel:

CERTIFICATE OF SERVICE

I hereby certify that on December 22, 2017, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to counsel of record and constitute service on such counsel and their represented parties pursuant to Fed. R. Civ. P. 5(b)(2)(E) and Local Rule 5.1(d).

/s/ Brett E. Lewis

Brett E. Lewis